CLAIMS

What is claimed is:

1. A method for creating a message digest from a message, wherein a sequence of input words is derived from the message, and the method comprises:

performing a portion of an operation, wherein the operation is a set of processes that operates on a word of the sequence;

performing a portion of a next operation in parallel with performing the portion of the operation, wherein the next operation is a set of processes that operates on a next word of the sequence; and

repeating performing the portion of the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence.

2. The method as claimed in claim 1, wherein the operation comprises:

performing a non-linear function on three of four variables stored in three of four registers;

adding an output of the non-linear function to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum;

circularly shifting the first sum by a number of bits, resulting in a shifted result;

adding the shifted result to contents of one of the four registers, resulting in a second sum; and

replacing contents of one of the four registers with the second sum.

3. The method as claimed in claim 2, further comprising:

temporarily storing the second sum, resulting in a stored sum, and

wherein replacing the contents of one of the four registers comprises replacing the contents with the stored sum.

4. The method as claimed in claim 1, wherein performing the portion of the next operation comprises:

performing a non-linear function on three of four variables; and

adding together the next word, a constant word, and a fourth variable of the four variables, resulting in a first sum.

5. The method as claimed in claim 4, further comprising performing remaining processes of the next operation after performing the portion of the next operation.

6. The method as claimed in claim 5, wherein performing the remaining processes comprises:

adding an output of the non-linear function to the first sum, resulting in a second sum;

circularly shifting the second sum by a number of bits, resulting in a shifted result; and

adding the shifted result to one of the four variables.

7. The method as claimed in claim 1, wherein when the operation is a first operation being performed on a first word of the sequence, the method further comprises:

performing a second portion of the operation before performing the portion of the operation.

8. The method as claimed in claim 7, wherein the second portion of the operation comprises:

performing a non-linear function on three of four variables stored in three of four registers; and

adding an output of the non-linear function to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum.

9. The method as claimed in claim 8, wherein the first portion of the operation comprises:

circularly shifting the first sum by a number of bits, resulting in a shifted result;

adding the shifted result to contents of one of the four registers, resulting in a second sum; and

replacing contents of one of the four registers with the second sum.

10. The method as claimed in claim 1, wherein performing the portion of the operation and performing the portion of the next operation are completed during a first clock cycle, and the method further comprises performing remaining processes of the next operation during a next clock cycle.

11. The method as claimed in claim 1, wherein performing the portion of the first operation is completed during a first clock cycle, and when the operation is a first operation being performed on a first word of the sequence, the method further comprises: performing a second portion of the operation during a preceding clock cycle.

12. The method as claimed in claim 1, wherein the message comprises one or more 512-bit blocks, each of which includes sixteen 32-bit words, and the message digest includes 128 bits.

13. The method as claimed in claim 1, wherein the message digest is identical to another message digest computed by MD5, given a same message.

14. A computer readable medium having computer executable instructions stored thereon for performing a method for creating a message digest from a message, wherein a sequence of input words is derived from the message, and the method comprises:

performing a portion of an operation, wherein the operation is a set of processes that operates on a word of the sequence;

performing a portion of a next operation in parallel with performing the portion of the operation, wherein the next operation is a set of processes that operates on a next word of the sequence; and

repeating performing the portion of the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence.

15. The computer readable medium as claimed in claim 14, wherein the operation comprises:

performing a non-linear function on three of four variables stored in three of four registers;

adding an output of the non-linear function to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum;

circularly shifting the first sum by a number of bits, resulting in a shifted result;

adding the shifted result to contents of one of the four registers, resulting in a second sum; and

replacing contents of one of the four registers with the second sum.

16. The computer readable medium as claimed in claim 14, wherein performing the portion of the next operation comprises:

performing a non-linear function on three of four variables; and

adding together the next word, a constant word, and a fourth variable of the four variables, resulting in a first sum.

17. The computer readable medium as claimed in claim 16, wherein the method further comprises performing remaining processes of the next operation after performing the portion of the next operation.

18. The computer readable medium as claimed in claim 17, wherein performing the remaining processes comprises:

adding an output of the non-linear function to the first sum, resulting in a second sum;

circularly shifting the second sum by a number of bits, resulting in a shifted result; and

adding the shifted result to one of the four variables.

19. The computer readable medium as claimed in claim 14, wherein when the operation is a first operation being performed on a first word of the sequence, the method further comprises:

performing a second portion of the operation before performing the portion of the operation.

20. The computer readable medium as claimed in claim 19, wherein the second portion of the operation comprises:

performing a non-linear function on three of four variables stored in three of four registers; and

adding an output of the non-linear function to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum.

21. The computer readable medium as claimed in claim 20, wherein the first portion of the operation comprises:

circularly shifting the first sum by a number of bits, resulting in a shifted result;

adding the shifted result to contents of one of the four registers, resulting in a second sum; and

replacing contents of one of the four registers with the second sum.

22. The method as claimed in claim 14, wherein performing the portion of the operation and performing the portion of the next operation are completed during a first clock cycle, and the method further comprises performing remaining processes of the next operation during a next clock cycle.

23. The method as claimed in claim 14, wherein performing the portion of the first operation is completed during a first clock cycle, and when the operation is a first operation being performed on a first word of the sequence, the method further comprises:

performing a second portion of the operation during a preceding clock cycle.

24. The computer readable medium as claimed in claim 14, wherein the message comprises one or more 512-bit blocks, each of which includes sixteen 32-bit words, and the message digest includes 128 bits.

25. The computer readable medium as claimed in claim 14, wherein the message digest is identical to another message digest computed by MD5, given a same message.

26. An integrated circuit for creating a message digest from a message, wherein a sequence of input words is derived from the message, and the integrated circuit comprises:

a first logic block which performs a portion of an operation during a clock cycle, wherein the operation is a set of processes that operates on a word of the sequence, performs a portion of a next operation during the clock cycle, wherein the next operation is a set of processes that operates on a next word of the sequence, and repeats performing the portion of the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence,

wherein additional passes through the first logic block are made until calculations have been performed that sequentially operate on all remaining words of the sequence.

27. The integrated circuit as claimed in claim 26, wherein the first logic block comprises:

a non-linear function block, which receives three of four variables; and

one or more first adders, which add together the next word, a constant word, and a fourth variable of the four variables, resulting in a first sum;

a second adder, which adds an output of the non-linear function block to the first sum, resulting in a second sum;

a shifter, coupled to the second adder, which circularly shifts the second sum by a number of bits, resulting in a shifted result; and

a third adder, coupled to the shifter, which adds the shifted result to one of the four variables.

28. The integrated circuit as claimed in claim 27, further comprising:

a multiplexer, coupled to the second adder, which passes the output of the non-linear function and the first sum to the second adder.

29. The integrated circuit as claimed in claim 26, further comprising:

a second logic block, coupled to the first logic block, which performs a second portion of the operation during a preceding clock cycle.

30. The integrated circuit as claimed in claim 29, wherein the second logic block comprises:

a non-linear function block, which receives three of four variables stored in three of four registers; and

one or more first adders, coupled to the non-linear function block, which add an output of the non-linear function block to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum.

31. The integrated circuit as claimed in claim 26, wherein the message comprises one or more 512-bit blocks, each of which includes sixteen 32-bit words, and the message digest includes 128 bits.

32. The integrated circuit as claimed in claim 26, wherein the message digest is identical to another message digest computed by MD5, given a same message.

33. An integrated circuit for creating a message digest from a message, wherein a sequence of input words is derived from the message, and the integrated circuit comprises:

a front computation logic block, which performs a portion of a first operation within a round of multiple operations during one or more clock cycles, wherein the first operation is a set of processes that operates on a word of the sequence; and

a systolic computation logic block, coupled to the front computation logic block, which performs a second portion of the first operation during one or more subsequent clock cycles, and performs a portion of a next operation during the one or more subsequent clock cycles, wherein the next operation is a set of processes that operates on a next word of the sequence, and the systolic computation block iterates until remaining operations within the round of multiple operations are completed.

34. The integrated circuit as claimed in claim 33, wherein the front computation logic block comprises:

a non-linear function block, which receives three of four variables stored in three of four registers; and

one or more first adders, coupled to the non-linear function block, which add an output of the non-linear function block to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum.

35. The integrated circuit as claimed in claim 33, wherein the systolic computation logic block comprises:

a non-linear function block, which receives three of four variables; and

one or more first adders, which add together the next word, a constant word, and a fourth variable of the four variables, resulting in a first sum;

a second adder, which adds an output of the non-linear function block to the first sum, resulting in a second sum;

a shifter, coupled to the second adder, which circularly shifts the second sum by a number of bits, resulting in a shifted result; and

a third adder, coupled to the shifter, which adds the shifted result to one of the four variables.

36. The integrated circuit as claimed in claim 33, wherein the message digest is identical to another message digest computed by MD5, given a same message.

37. An electronic device comprising:

an integrated circuit, which creates a message digest from a message, wherein a sequence of input words is derived from the message, and the message digest is created by performing a portion of an operation, wherein the operation is a set of processes that operates on a word of the sequence, performing a portion of a next operation in parallel with performing the portion of the operation, wherein the next operation is a set of processes that operates on a next word of the sequence, and repeating performing the portion of the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence.

38. The electronic device as claimed in claim 37, wherein the integrated circuit is a processor, and the electronic device further comprises:

a computer readable medium, coupled to the integrated circuit, which has computer executable instructions stored thereon that cause the processor to perform the portion of the operation, perform the portion of the next operation, and repeat performing.

39. The electronic device as claimed in claim 37, wherein the integrated circuit comprises:

a first logic block, which performs the portion of the operation during a clock cycle, performs the portion of the next operation during the clock cycle, and repeats performing the portion of the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence.

40. The electronic device as claimed in claim 39, wherein the integrated circuit further comprises:

a second logic block, coupled to the first logic block, which performs a second portion of the operation during a preceding clock cycle.

41. The electronic device as claimed in claim 37, further comprising:
an external interface, which transmits the message digest.

42. The electronic device as claimed in claim 37, further comprising:
an external interface, which transmits data that was generated from the message digest.